Tests have been conducted by both organizations to determine performance of their system components.

It is reported that most of the radio traffic will be in-bound, meaning from the mobile to the base station [17]. Severe radio environments, such as the Chicago hub, exist where many mobiles may be contending for the same base station, interference from other signal sources may be greater than normal, and propagation effects due to the urban environment may be more demanding of the radio system than normal. No known simulations have been conducted for the ATCS to determine the radio system performance in severe radio environments with many mobiles contending for the base station.

Matrix Element Evaluation *Hardware simulators of the radio channel and environment have been developed by equipment manufacturers to test their system components. Analyses of radio communications in the ATCS have been completed to determine radio channel capacity under defined conditions. Simulation studies should be conducted to determine the ATCS radio system performance in severe environments with many mobiles contending for the base station.*

5.5.3 Field Tests - Range of Environments

A field test provides a situation where the proposed system is linked with live or operational equipment that the system will eventually support, while the live equipment operates in the environment that is its domain. In a field test, ultimate control usually resides with the human operators of the live equipment, allowing the operators to respond to and correct any mistakes made by the system under test. Field testing is the next step in test and validation of a proposed system after simulation studies. Laboratory hardware and computer software simulation techniques can never totally replace the environment of the live equipment.

AMCI and Union Pacific have implemented portions of the ATCS on Union Pacific track to control Work Order processing. Canadian National has attempted limited tests of the ATCS on a section of their track. Others have tested functions of the interrogators/transponders under a variety of conditions or have tested limited features of the ATCS on selections of track. Rockwell and Burlington Northern did a considerable amount of testing of the Advanced Railroad Electronic System (ARES) project on the Iron Range section of Burlington Northern track. All of these tests provide confidence builders and valuable information for improving portions of the ATCS. However, no known full-function ATCS testing on an operational field test is planned.

It is human nature to rely on the results of live demonstrations of systems in operation, beyond the simulation stage, before we humans can put faith and trust into a new system. A field test program of a fully-functioning ATCS will need to be initially demonstrated in a non-hostile, less stressful environment. The purpose of field testing is to discover and correct system problems in order to improve the system before a larger implementation begins. A system that has been demonstrated to work in a field test would next be introduced into a more hostile environment. This expanded field

test is known as a pilot demonstration and is larger in scope and would probably involve a transportation corridor to demonstrate the ATCS.

On April 29, 1994, the Union Pacific and Burlington Northern Railroads issued press releases outlining their joint project to develop and test the feasibility of electronic train monitoring and control systems under what they call "Positive Train Separation", PTS. The PTS multi-year test project will be conducted on both Union Pacific and Burlington Northern tracks in Washington and Oregon, where the two railroads have connecting and parallel track. The PTS project will share many of the features of the ATCS as Union Pacific has installed ATCS-compliant equipment on much of its track, and the PTS project could have new features based upon knowledge gained by Burlington Northern with its ARES field trials.

Matrix Element Evaluation *Some individual railroads have begun testing different features of the ATCS. A coordinated effort is required to field test a full implementation of the ATCS on a section of track with typical environmental conditions. A more comprehensive field test or pilot demonstration would be required to show that the ATCS can properly function in more severe environments such as the Chicago hub or the Northeast corridor.*

5.6 Migration

5.6.1 Implementation and Replacement Plan for Each Current System (Railroad)

Migration provides for the orderly transition from one system to another. It is a step-by-step plan to phase out one system for another. Businesses rarely can shut down one system and immediately start up another. In many cases the two systems are operated in parallel. Parts of a business may convert to the new system before other parts are able to start their conversion.

The AAR/RAC has recently formed a committee to investigate migration. Discussions on migration were presented at the September 1993 meeting on the ATCS in Baltimore. Firm migration plans are still to be developed.

Migration also includes a timetable for the conversion process. The timetable accounts for the acquisition of funding, the installation and testing of ATCS equipment, and training for users of the new system.

Matrix Element Evaluation *Without a clear migration path and associated timetable, the benefits of positive train separation provided by the ATCS could be greatly delayed. The migration plan and timetable should seek to accommodate all railroads, and to encourage widespread use of the ATCS in the shortest time schedule possible.*

5.6.2 Continuous Protection During Migration

As discussed in the preceding section, systems are rarely implemented overnight to replace existing systems. Each railroad will need to operate its present safety system simultaneously with the ATCS it is implementing. After the ATCS implementation is complete and thoroughly tested, the railroad would phase out and remove its existing control system.

Different railroads may not implement the ATCS elements needed for safety, or they may not implement them on the same time schedule as other railroads that are implementing full ATCS. Because the railroad industry allows equipment of one railroad to be operated on the tracks of another railroad, a safety issue could develop if existing control systems were removed too soon.

The experience gained from the PTS pilot project will provide knowledge on how to proceed with current safety features while implementing the new safety features obtained through the PTS project. Other railroads will be able to learn from the Union Pacific and Burlington Northern experience and knowledge.

Matrix Element Evaluation *The migration plan needs to ensure that safety measures already in place are not removed before all trains that pass through the territory have suitably-equipped ATCS locomotives. Older systems and the ATCS will probably have to be operated in parallel while the ATCS becomes fully operational for all railroads providing track to other rail industry users.*

5.7 Management

5.7.1 Conflict Resolution

Conflict resolution commonly refers to situations where two or more entities claim that they control the same address or that they have the same address. For instance, two different CCs might claim responsibility for the same train. In this situation, both CCs would attempt to have traffic addressed to that train routed through each controller. Or, two trains, incorrectly identified with the same address, conceivably could be provided with the wrong commands. The system logic needs to understand how to handle these situations. Failure to properly deal with conflicts could have serious results.

The approach taken by the ATCS to handle and prevent this sort of problem is multi-leveled. The first level approach is an attempt to prevent such a circumstance. The second level is to design control flows to correct such a problem. The third level is to ensure that authorizations limit movement of trains.

Prevention is the first level and probably the most elaborate process in the ATCS's conflict resolution scheme. The address of each train, and track force vehicle is "hard coded" into the device. Hard

code means that the address is non-changeable. Additionally, the reliability specifications demand that the probability of any device transmitting the incorrect address is 10^{-9}.

At the second level, control flows work to prevent such an contention through at least three different processes. First, there is an elaborate "hand-shaking" between CCs before train responsibility is provided to one of the controllers. Hand-shaking is defined as a hardware or software sequence of events requiring mutual consent of conditions prior to the change [6]. The second process involves the message information. All messages which a train sends forward contain the authority under which that train is operating. If the authority reported by the train is different from that recorded by the dispatch computer, the train should stop immediately. The third process consists of the train's on board computer checking with each switch as the switch is approached. In this manner the switch setting and the authority number are verified. Any discrepancies result in the train stopping.

The third level which helps prevent collisions in the event of some conflict between nodes is the issuance and content of movement authorities. Before a safety computer allows a dispatch computer to issue a movement authority, the safety computer records the train address (ID) and the track assigned by the authority. The computer also certifies that there are no previously issued authorities which will conflict.

Matrix Element Evaluation *The ATCS addresses the possibility of conflicts. Conflicts are expected to occur on establishing control between nodes and with improperly transmitted addresses. These conflicts are to be resolved by well-planned control flows. This demonstrates the need for the validation of control flows.*

5.7.2 Hand-off Between Nodes (Cluster Controllers)

In a communications network where some of the stations are mobile, there is a need for the system to hand-off, transfer control of a mobile station from one base station to another, as the mobile station moves. Radio-based systems add to the degree of hand-off difficulty because the signal reception can vary in amplitude as the mobile station moves. As the received signal level from the mobile transmitter varies in amplitude at two adjacent base stations, there is the potential for transferring of the mobile station back and forth between the two base stations unless some procedure prevents this occurrence.

A protocol must be established and tested that allows a smooth transfer from one base station to the other to occur as the mobile station moves. Issues such as signal strength, conflict resolution, addressing, and management responsibility must be addressed and resolved. The consequence of not establishing a proper hand-off procedure can result in unwanted responses, such as freezing trains in place, "losing" control of a train, or generating so much traffic that the system reaches congestion collapse.

Hand-off procedures are described in Specification 200, Figure R-1. In a brief summation, the base station computer/radio, called the base controller package (BCP), reports that it has detected the transmission of a data message from a train's mobile radio station. Then the BCP's cluster controller, CC (A), announces to other CCs that it is receiving train X, and CC (A) checks to see if another CC controls train X. CC (B), currently controlling the train, tells CC (A) that it is controlling train X. The two CCs check signal strength until the train is stronger in CC (A) territory. The CCs jointly control the train until the train is completely in A's territory. At this point CC (A) announces that it is now the controller of train X. The procedures defined in the hand-off specification are typical of other operations to be performed by the ATCS.

Matrix Element Evaluation *The system developers have provided a considerable effort to detail the hand-off procedure between base stations, cluster controllers, etc. The concern remains in how the procedures are to be verified in real-world circumstances.*

5.7.3 Protection from Threats

In a data communications system, a threat is any possible or conceivable intrusion into or against the system which either disrupts operations or causes the system to act in a manner other than its intended functionality. In terms of the railroad control system, a threat could be defined as anything from tampering with a switching device to breaking into the system and generating false messages. The threats may include deliberate intruders (like terrorists) or accidental ones (like careless employees). To properly address the concern of threats the user must conduct a threat analysis, evaluate each threat and then determine which threats need to be mitigated through hardware/software design or through modified procedures

The ATCS addresses threats through a variety of different methods. A "Security Threat Summary" is contained on page 3-27 of Specification 200. Developers of the specification indicated that their threat analysis showed a very low threat probability, and further investigation is not required.

Matrix Element Evaluation *An ATCS threat survey has been conducted and potential solutions are contained within the specifications. Completeness of the threat analysis in Specification 200 can not be determined from material available to ITS. A literature search did not reveal any additional threat studies. Modeling of system performance and the potential impact of intrusions into the ATCS network could indicate a need for a more detailed threat analysis.*

6. CONCLUSIONS

The Advanced Train Control System is a development project of two railroad associations, the Association of American Railroads and the Railways Association of Canada. The ATCS' purpose is to provide enhanced control of train movement with a common set of operating procedures and system performance requirements across all railroads in North America The ATCS implements and

automates the safe operating procedures, presently practiced by the railroads, to help railroad personnel perform their responsibilities in a safe manner. The system specifications are intended to allow open competition among all vendors, while ensuring compatible and interoperable operation of the system components.

The ATCS, as a set of specifications, have been developed from a well-planned open forum of railroad specialists, system designers, and equipment manufacturers. The ATCS follows established, safe operating procedures to aid railroad personnel in their decision-making and actions in the movement of trains. The ATCS uses techniques that have been well tested by other systems to ensure the validity, accuracy, and timeliness of the data sent from the data source to the data receiver. The ATCS conducts self-tests to determine equipment faults and provides a means to recover from the failures. When the ATCS begins to fail, the system alerts the human operators of the conditions while maintaining as much of the data communications as possible. The system operates in a fail-safe manner, in the event the ATCS suffers a complete failure, operators and other components of the system are notified and the decision-making control is yielded to human operators. Finally, the ATCS will allow for expansion of capabilities as new technology or new operating techniques develop in the years to come.

A collision avoidance system provides the means of detecting and preventing impending collisions between vehicles. The ATCS has the ability to provide collision avoidance or positive train separation between ATCS-equipped trains operating on ATCS-equipped track. The significant factor in the statement is "ATCS-equipped", which can mean anything from a very limited implementation of the ATCS to a full implementation. However, anything less than full implementation of the safety features provided by the ATCS may not result in positive train separation.

Additional ATCS development effort is required, or at least desirable, in the following areas:

- The ATCS specifications implement safe railroad operating procedures through computer and communication hardware and software to assist railroad personnel in following the procedures. Those ATCS specifications which define all the steps required to carry out the procedures are called control flows. Because of the complexity of the control flows and because correct control flows are essential to safety, ITS recommends independent modeling and validation of the ATCS control flows under a variety of operating scenarios to ensure that the system functions as intended.

- Various railroads and railroad equipment manufacturers have implemented portions of the ATCS or have conducted limited tests of the ATCS system components. A coordinated effort is required to field test a full implementation of the ATCS safety features on a section of track with typical environmental conditions. The results of the testing could be used to further improve the control flows and system specifications. A more comprehensive test should follow in a more severe environment, such as the Northeast corridor or the Chicago hub. A pilot demonstration in the severe environment will build

confidence in the system capabilities as well as provide information to further improve the system specifications.

- A migration plan and a timetable for full ATCS implementation is needed. The migration plan will allow for an orderly transition from present control systems to the ATCS. It is important that presently available safety features are not disabled while the ATCS is installed. The present ATCS implementation plan allows railroads to adopt any level of the ATCS they desire. As noted in the ATCS specification documentation, the ATCS will be at the lowest capability of either the equipment or track at any instant. For example, ATCS-equipped trains on non-ATCS equipped track will not provide ATCS safety; neither will non-ATCS equipped trains on ATCS-equipped track. The implementation timetable accounts for the acquisition of funding, the installation and testing of the ATCS equipment, and training for users of the new system. The timetable should seek to accommodate all railroads to encourage widespread use of the ATCS at its fullest safety capability level.

A press release on April 28, 1994, by the Union Pacific and Burlington Northern Railroads indicated the start of a joint project between the two railroads to develop the Positive Train Separation system with a pilot test program to be conducted on Union Pacific and Burlington Northern track in the Pacific Northwest. The preliminary descriptions of the joint project provide insight as to the scope of the effort. Many of the ATCS features will be retained with potential new ones added. The field tests and migration experiences will provide much of the knowledge requested in the last two recommendations listed above.

7. REFERENCES

[1] *Rail Safety Enforcement and Review Act of 1992*, Public Law No. 102-365.

[2] Association of American Railroads and Railways Association of Canada, *Advanced Train Control Systems, Specifications*, prepared by and available from ARINC Research Corporation, Washington DC. Major Specifications are:

ATCS Specification 100, System Architecture Overview, Rev. 3.0 Mar. 1993
ATCS Specification 200, Communications Systems Architecture, Rev. 3.0 Mar. 1993
ATCS Specification 300, Locomotive System Architecture, Rev. 3.0 Mar. 1993
ATCS Specification 400, Dispatch System Architecture, Rev. 3.0 Mar. 1993
ATCS Specification 500, Field Systems Architecture, Rev. 3.0 Mar. 1993
ATCS Specification 600, Work Vehicle System Architecture, Rev. 3.0 Mar. 1993

[3] D. C. Coll, A. U. H. Sheikh, R. G. Ayers, and J. H. Bailey, "The communications system architecture of the North American Advanced Train Control System", *IEEE Trans. Veh. Technol.* 39, No. 3, Aug. 1990, pp. 244-255.

[4] International Telecommunications Union - Telecommunications Sector (ITU-T, formerly CCITT), *Data Communication Networks: Open System Interconnection (OSI) - Model and Notation, Service Definition*, CCITT Recs. X.200-X.219, Fascicle VIII.4, IXth Plenary Assembly, Melbourne, 1988.

[5] A. U. H. Sheikh, D. C. Coll, R. G. Ayers, and J. H. Bailey, "ATCS: Advanced Train Control System radio data link design considerations", *IEEE Trans. Veh. Technol.* Vol. 39, No. 3, Aug. 1990, pp. 256-262.

[6] Institute of Electrical and Electronics Engineers, *The New IEEE Standard Dictionary of Electrical and Electronics Terms*, IEEE Std 100-1992, ISBN 1-55937-240-0, IEEE, Inc., NYC, NY.

[7] R. G. Ayers, "Selection of a forward error correcting code for the data communication link of the Advanced Train Control System", *IEEE Trans. Veh Technol.*, Vol. 38, No. 4, Nov. 1989, pp. 247-255.

[8] S. Adler, "A public safety digital system development", *APCO Bulletin*, Apr. 1993.

[9] Association of American Railroads, "Locomotive system integration architecture specification", Ver. 3.0, Jan. 1993, prepared by and available from ARINC Research Corporation, Washington DC.

[10] W. Stallings, *Data and Computer Communications*, Third Edition, Macmillan Publishing Co., New York, 1991.

[11] Frasco and Associates, Inc., ATCS EMI/EMC program reports:
"Task 1, Interim progress report", Jan. 1989.
"Task 2, Final progress report, preliminary EMI testing", Jan. 1989.
"Task 3, Final progress report, preparation and testing of ATCS EMI test procedures", Jan. 1989.
"Task 3, Test data appendix", Jan. 1989.
prepared for and available from ARINC Research Corporation, Washington DC.

[12] J. L. Haselwood, "Comparison of life cycle costs UHF and VHF data radio networks", Battelle prepared for Association of American Railroads, Sept. 1992.

[13] A. Mautschke, E. Furman, and R. Decker, "Mobile data transmission in a railroad environment", IEEE Veh. Technol. Conf. 1990, (also available as P/N T03002 from Automated Monitoring and Control International, Inc. Omaha, NE, 68164).

[14] G. A. Hufford, A. G. Longley, and W. A. Kissick, "A guide to the use of the ITS Irregular Terrain Model in the area prediction mode", NTIA Report 82-100, Apr. 1982 (Available from National Technical Information Service, Order No. PB82-217977).

[15] Institute for Telecommunication Sciences, "Communication System Performance Model - CSPM", available through TAServices, an on-line set of computer models, contact TAServices Support at ITS, Boulder, CO, ph. (303) 497-3500.

[16] E. L. Furman, "Performance and capacity analysis of an operating ATCS communication system", P/N T03008, Automated Monitoring and Control International, Inc. Omaha, NE, 68164, 1991.

[17] H. Sharif and E. Furman, "Analytical model for ATCS inbound RF channel throughput", Automated Monitoring and Control International, Inc. Omaha, NE, 68164, 1991.

[18] W. W. Weinstein and A. L. Schor, "Safety analysis of the ATCS", CSDL-R-2098 (Rev. 1), The Charles Stark Draper Laboratory, Inc., Cambridge, MA 02139, 1990.

[19] R. E. Kalman, "A new approach to linear filtering and prediction problems", *Journal of Basic Eng.*, 82, March 1960, pg. 34-45.

[20] C. V. Negoita, *Expert Systems and Fuzzy Systems*, Benjamin/Cummings Publishing Co., Inc., Menlo Park CA, 1985

Appendix 3

Background Note: PTC Criteria and Technological Alternatives

Chapter IV of this report describes the history of automatic train control (ATC) systems and similar safety systems (ATS, ACS) in the United States. In general, the most active phase of ATC installation coincided with high frequencies of intercity rail passenger service. A variety of ATC systems continue to be employed in the United States and internationally.

The purpose of ATC is to stop the train or reduce its speed to the prescribed rate if the crew member fails to acknowledge and/or obey the more restrictive indication within the prescribed time. These and similar systems have long been recognized as necessary to assure safe operations of trains at high speeds. Although this report uses PTC to describe a range of technology that includes signal-based ATC and other systems, contemporary ATC systems remain among the most capable alternatives to promote safety.

From a regulatory standpoint, requirements for train control in the United States are presently based exclusively on speed. The speed provisions contained in 49 CFR § 236.0 (which require ATC, ATS or cab signals above 79 miles per hour) have remained unchanged since being issued in 1947. Different speeds, both higher and lower, were suggested at the time the order was being considered. During the interim years there have been recommendations to both raise and lower the speeds. As this report was being finalized, FRA received a petition for rulemaking from a rail labor organization that would require the latter.

Train density has been suggested as an alternative criterion for deployment of PTC systems. In fact, the number and temporal spacing of train movements is employed as an evaluation criterion by FRA when railroads seek to discontinue signal systems of all kinds. Factors that may be pertinent to PTC requirements include number and kinds of trains in a specific time frame, as well as speed. Although density, as such, is not currently a regulatory criterion for deployment of ATC or other positive train control technology, it is definitely a practical consideration with respect to the cost effectiveness of more capable train control systems. Recently, for instance, the Florida East Coast Railway installed a new ATC system on its heavily used main line in Florida.

The signal and train control system characteristics required in Europe for speeds between 100 and 125 mph are broadly similar to the FRA requirement for speeds of 80 mph and over. The principal difference is that in the U.S., all trains operating on a line equipped with cab signals and/or ATC are required to meet the minimum requirements. In Europe, only high speed trains are required to meet the minimum requirements. This distinction is without meaning, of course, on those lines dedicated to very high speed passenger operation.

New train control systems in Europe, Japan and North America make extensive use of microprocessors. New applications for high speeds invariably provide for all or most of the features of positive train control. However, technical approaches differ.

On the French TGV Atlantique Line, the train operator controls the train, relying on input received from the cab signal system. Information for the cab signal system can be received from up to 18 ac audio-frequency coded track circuits. Information from the cab signal system includes the speed limit of the current block and the speed required by the end of the following block. The TGV has an automatic braking system that stops the train when the operator exceeds the speed limit.

In Germany, the ICE train utilizes computers for vital safety-critical information and control elements of the automated control system. Three operational methods are available: (1) fully automated speed control; (2) manual selection of speeds, allowing the speed control to meet the preselected speed; and (3) full manual operation, utilizing control system information on the console for guidance. Communication between the train and right of way is provided by inductive loops in the gage of the track (a communication method also employed in Austria and Spain).

European planners are working toward a network of high speed railroads that may eventually utilize a common ATC system. The extent to which lower speed lines used for mixed passenger and freight traffic might be affected by this development is not presently known.

INTENTIONALLY

LEFT BLANK